



Staatstrojaner

Überwachung Am quibusdaes autem harunt, quattuor estem euer? Ihillo et aut rernam, sa venihic te pos sunt, arunt quo es namus il in nonsed magna de int, utes sa consed mo tem comnisquos quam estiam, vendust experum quibuscime ra volor ape dolestia cus, solupta tatemqui num quamus apictor esequaecto eaquiasum quias quae. Luptatem idundae perrum aut eosse nisim quae oficit et as et aliaeri amusdandi blam, nim sam haruptatibus aut.

Jens Seipenbusch

„Wenn die Regierung normale Bürger beobachtet, die nicht eines Verbrechens verdächtig sind, ist dies eine fundamental inakzeptable und klare Verletzung des Bürgerrechts auf Privatsphäre.“ So steht es 2006 in der Grundsatzklärung der schwedischen Piratenpartei. Und dann auch noch später: „In allen anderen Fällen sollte die Regierung annehmen, ihre Bürger seien unschuldig, und sie in Ruhe lassen. Diesem Kommunikationsgeheimnis muss ein starker gesetzlicher Schutz gegeben werden, da die Regierung wiederholt gezeigt hat, dass sie bei sensiblen Informationen nicht vertrauenswürdig ist.“

Doch was ist so besonders am ersten Jahrzehnt des neuen Jahrtausends, dass die Piraten die Privatsphäre der Bürger so stark bedroht sehen und dem Staat gleichermaßen pauschal eine die Bürgerrechte unterminierende Vorgehensweise unterstellen? Die beiden Hauptursachen dafür kann man sich gut am Beispiel des sogenannten ‚Staatstrojaners‘ (oder ‚Bundestrojaners‘, ‚Landestrojaners‘) vor Augen führen. Diese Na-

men haben sich für ein Stück Software eingebürgert, das den Behörden eine sogenannte Online-Durchsuchung ermöglicht, eine Maßnahme um „entfernte PCs auf verfahrensrelevante Inhalte hin zu durchsuchen, ohne tatsächlich am Standort des Gerätes anwesend zu sein“, wie es im ‚Programm zur Stärkung der Inneren Sicherheit‘ der deutschen Bundesregierung von 2006 umschrieben wird. Damit ist zunächst einmal die heimliche Durchsuchung des Datenbestandes auf dem Computer eines Verdächtigen möglich, sozusagen der nächste Schlag gegen die Unverletzlichkeit der Wohnung, nachdem in den Jahren zuvor erst der große Lauschangriff eingeführt wurde (CDU/CSU/FDP). Der große Lauschangriff, die optische oder akustische Wohnraumüberwachung durch Strafverfolgungsbehörden und Nachrichtendienste, nahm in Deutschland bereits 1998 seinen Lauf als Grundgesetzänderung, bevor er dann aufgrund des Urteils des Bundesverfassungsgerichts modifiziert werden musste und schliesslich 2005 endgültig umgesetzt wurde. Nachdem hier-

mit also bereits ein verfassungsrechtliches Loch in die zuvor verbriefte Privatsphäre innerhalb der eigenen vier Wände gebohrt worden war, erstreckten sich die Begehrlichkeiten naturgemäß auch auf die zunehmend digital vorliegenden Dokumente und Informationen auf privaten Computern. Ähnlich wie auch in vielen anderen Bereichen der digitalen Revolution erfolgte die rechtliche Diskussion reaktiv: konnte man eine heimliche Online-Durchsuchung überhaupt mit einer normalen Hausdurchsuchung vergleichen, musste gar eine ganz neue gesetzliche Grundlage her? Parallel dazu entsteht 2001 die andere große treibende Kraft des Bürgerrechtsabbaus: mit den für Teile der westlichen Welt traumatisierenden Anschlägen von 9/11 auf das World Trade Center in den USA tritt die Bekämpfung des Terrorismus als neues vorrangiges, globales, sicherheitspolitisches Ziel in den Vordergrund und beendet damit eine recht kurze Übergangszeit der Frontenlosigkeit nur ein gutes Jahrzehnt nachdem der kalte Krieg durch den Beitritt der DDR zur BRD praktisch zu Ende gegangen war.

Der damalige deutsche Innenminister Schäuble formulierte diese Veränderung vor wenigen Jahren in etwa so: man müsse als Staat in Zukunft nicht mehr zwischen innerer und äußerer Sicherheit unterscheiden. Die Terrorismusbekämpfung als Leitlinie der inneren Sicherheit hat dabei zwei fatale Aspekte: zum einen ist Terrorismus primär eine Kommunikationsstrategie. Man spielt ihr voll in die Hände, wenn man diese Verbrechen entweder überhöht in den Medien darstellt oder auch mit drakonischen Sicherheitsmaßnahmen beantwortet. Alles was der Verbreitung des Schreckens dient, nützt den Terroristen. Zum anderen ist der Terrorist als gesuchte Zielperson vor seinem Anschlag strukturell oft kaum oder gar nicht von einem normalen Bürger zu unterscheiden. Auch deswegen gilt heute die Devise „jeder ist verdächtig“ leider allzu oft. Auch deswegen ist die Politik heute so anfällig gegenüber den maßlosen Begehrlichkeiten von Polizei und Geheimdiensten hinsichtlich einer allumfassenden Überwachung. Und hier kommen wir dann zurück zum Staatstroja-

ner. Denn die herkömmliche Überwachung von Telekommunikation ist in der heutigen Zeit von verschlüsselten Internet-Telefonie-Diensten und entsprechender Software nicht mehr so einfach wie früher. Wo das ‚Lauschen am Draht‘ so gar nicht mehr funktioniert, sehen einige Behörden schon einen derartigen Abhör-Notstand, dass sie eine sogenannte Quellen-TKÜ verlangen. Das ist eine Telekommunikationsüberwachung, die dort mithört, wo der Verdächtige seine verschlüsselte Kommunikation beginnt: auf seinem Computer. Der Staatstrojaner soll dann diese Informationen abgreifen, bevor die Software die Daten verschlüsselt und übermittelt, sei es Text oder Gespräche.

Insgesamt sind es also zwei Erfolgsfaktoren der technischen Entwicklung, die hier von den Sicherheitsbehörden überkompensiert werden sollen. Der vernetzte Heimcomputer mit seinem digitalen Datenbestand als verlockender Honigtopf für Ermittler und Geheimdienste. Und dann die abhörsichere Verschlüsselung von Kommunikation, mit der der Bürger sein Recht auf Vertraulichkeit erstmals über längere Distanzen selbstständig garantieren kann. Beides ist ein rotes Tuch für die Überwacher. Mit dem Staatstrojaner begeben sich die Behörden aber erstmals selbst auf unbekanntes Terrain in der Informationsgesellschaft. Der allfällige Kontrollverlust zeigt sich hier zunächst darin, dass dieses delicate Instrument nicht etwa innerhalb der Behörden selbst entwickelt wird. Nein, man kauft die Software einfach ein. Nun ist es ein Unterschied, ob ich beispielsweise eine Palette Kopierpapier einkaufe oder ob ich ein Stück hochkomplexe Software einkaufe. Wer sich die detaillierten Ausführungen des Chaos Computer Club (CCC) in seiner Analyse des Bayerntrojaners anschaut, bemerkt dies sofort. Und so ist es kein Wunder, dass unter dem Stichwort ‚Ozapftis‘ herauskommt: die Software kann so einiges, was sie nach Recht und Gesetz gar nicht können dürfte. Staatliche Überwachung drängt mit Macht



ins digitale Zeitalter, leider ohne sich über die notwendigen Anpassungen der eigenen Vorgehensweise und des eigenen Selbstverständnisses Gedanken zu machen. Und leider oft genug auch ohne Kompetenz.

Diese Grundproblematik durchzieht alle Bereiche der Bürgerrechte. Als symptomatisch hierfür kann gelten, dass das Bundesverfassungsgericht nach dem ‚Recht auf informationelle Selbstbestimmung‘ nun 2008 das ‚Grundrecht auf digitale Intimsphäre‘ als Antwort auf die neuen Herausforderungen entwickelt hat – und nicht zuletzt auch als direkte Antwort auf den Anspruch der Sicherheitsbehörden, in private Computer einzudringen und hemmungslos mitzulesen.

Diese beiden Begriffe, ‚informationelle Selbstbestimmung‘ und ‚digitale Intimsphäre/Pri-

vatsphäre‘ geben uns heutzutage auch die Richtung an, in die sich moderner Datenschutz entwickeln muss, ganz unabhängig von den konkreten Ausprägungen. **Diese Ausprägungen stehen in der Tat ebenfalls vor enormen Herausforderungen im Informationszeitalter.** Aber warum ist es überhaupt wichtig, selbst im Zeitalter global vernetzter Informationsströme und weltöffentlicher sozialer Netzwerke irgendwelche Daten zu ‚schützen‘ und kann das überhaupt gelingen? **Es kann, und es ist eben nicht nur wichtig, die Daten zu schützen, sondern auch die Menschen, und deshalb ist es auch von überragender Bedeutung für eine menschenwürdige Informationsgesellschaft.** Informationen über Menschen bedeuten immer auch Macht. Einzelne Daten vielleicht weniger – obwohl schon eine einzige Information bereits heute darüber entscheiden kann, ob man

einen bestimmten Arbeitsplatz oder eine Versicherung oder einen Kredit bekommt oder eben nicht – auf jeden Fall aber die Kombination von unterschiedlichen Daten über eine Person. Im übrigen muss diese Information nicht mal richtig sein, um sich auszuwirken, gerade falsche Informationen können viel Macht über einzelne Menschen haben. Und sie muss auch gar nicht als Entscheidungsgrundlage bekannt oder benannt werden, um Macht zu entfalten, ja sie muss einen heutzutage nicht einmal direkt betreffen um Macht über einen zu haben. Beim sogenannten Scoring wird beispielsweise meine eigene Kreditwürdigkeit auch danach bewertet, wie die Zahlungsmoral meiner Nachbarn im Viertel ist. Ein besonders perfider Auswuchs von Datenmissbrauch, weil er dazu einlädt, sich ein Wohnviertel mit durchgängig gehobenem Anschein zu suchen, also zu sozi-

Stasi 2.0 - Das Leben der Anderen: Bundestrojaner und Konsorten haben das Zeug dazu, Bürger auszuspiionieren und ihnen im Falle eines Falles sogar Belastungsmaterial unterzuschieben. Das Ministerium für Staatssicherheit der DDR hätte seine helle Freude an dieser Technik gehabt.

(Foto: Buena Vista)

aler Segregation. Ähnliche Sippenhaft droht durch unbedarfte Nutzung sozialer Netzwerke. Wird der Nutzer beispielsweise dazu angehalten, seine elektronischen Adressbücher und Kontakte zum Auffinden von Freunden zur Verfügung zu stellen, dann nimmt das Netzwerk allzuoft die ganze Hand statt des kleinen Fingers und legt auch für diejenigen eine digitale Akte an, die es in den eigenen Datenbanken nicht vorfindet. Zu den üblichen Verdächtigen aus Staat und Wirtschaft tritt im Web 2.0 dann auch noch ein weiterer, ständig wachsender Faktor hinzu: die Nutzergemeinschaft mit ihrem sogenannten ‚user generated content‘, also beispielsweise private Blogs, Webseiten und Foren. Bei den sozialen Netzwerken überschneiden sich die Verantwortlichkeiten des Plattformbetreibers mit denen der Nutzergemeinschaft sehr stark. Hinzu kommen die allge-

meinen Besonderheiten von digitalen Daten: sie sind einerseits besonders flüchtig, also leicht zu verbreiten, leicht zu löschen aber auch leicht in der U-Bahn auf einem Datenträger zu verlieren, und andererseits besonders langlebig, wenn sie einmal veröffentlicht worden sind, sei es, dass sie ihren Weg in andere Teile des Internets gefunden haben, oder einfach archiviert worden sind von unterschiedlichen Interessenten.

Bei all dieser neuen Unübersichtlichkeit darf man aber nicht vergessen: der Datenschutz hat primär ein Umsetzungsproblem, keines der Definition. Es sind Menschen, Firmen und Behörden, die Daten speichern und veröffentlichen und damit Macht über den Einzelnen haben. Es ist nicht ein abstraktes ‚Internet‘ und es sind auch keine unbekannten Mächte, die die Handlungsfreiheit von

Menschen damit einschränken. Darüberhinaus müssen wir die neuen Probleme ja auch nicht mit alter Technik lösen. Im Gegenteil bringt Software an sich sogar quasi unbegrenzt viele Mittel zur Lösung von Problemen mit digitalen Daten mit. Mit Suchmaschinen kann ich auch die Daten über mich auffinden, die ich vielleicht anschliessend dann dort gelöscht haben möchte. Mit digitaler Zertifikatsverwaltung könnte ich automatisch und ohne dass er das verhindern kann protokollieren, welcher Behördenmitarbeiter sich wann welche Seite meiner digitalen Akte angesehen hat und ich könnte sogar automatisch darüber benachrichtigt werden. Transparenter Staat statt gläserner Bürger.

Bei der Lösung der Durchsetzungsproblematik stehen wir leider noch ziemlich am Anfang. Wenn schon ein deutsches

Gericht daran scheitert, für einen Prozess das facebook-Profil eines Beschuldigten (und inzwischen Verurteilten) anzufordern, obwohl die Firma sogar in Deutschland ansässig ist (und europaweit in Irland ihre Zentrale hat), dann sieht man, dass hier vor allem auf rechtlichem Gebiet noch einiges getan werden muss, bis man von einem rechtsstaatlich angemessenen Niveau bezüglich der Durchsetzung von bürgerrechtlichen Ansprüchen sprechen kann. Zu einem Durchbruch könnte uns dabei die neue EU-Verordnung zum Datenschutz verhelfen, die die EU-Kommissarin Reding vor kurzem mit einem guten Ausgangsentwurf auf den Weg brachte. Exemplarisch seien daraus zwei wichtige Neuerungen erwähnt, die Höhe von Strafzahlungen und den Gebietsbezug. In der Vergangenheit waren Geldstrafen bei Datenschutzvergehen für Unternehmen eine

INTERVIEW



Wir reden mit Dirk Schatz, Listenkandidat für die Landtagswahlen in NRW, und beruflich Polizeikommissar, über das Thema Staatstrojaner.

Das Interview führte Andreas Bogk.

? *Es gab ja im letzten Jahr im Herbst einen Vorfall, der Chaos Computer Club hat eine Trojanersoftware analysiert und veröffentlicht, die durch die Strafverfolgungsbehörden, unter anderem auch in NRW, eingesetzt wurde. Dabei wurde festgestellt, daß diese Software sich nicht im Rahmen des rechtlich zulässigen bewegt hat. Wie siehst du die damaligen Ereignisse?*

Ich bewerte das schon äußerst kritisch, vor allem, wenn man bedenkt, dass die eingesetzte Software eben nicht den gesetzlichen Grundlagen entsprach. Der Bundesgerichtshof hat festgestellt, dass es im Bereich der Strafverfolgung gar nicht zulässig ist, diese Software einzusetzen. Und im präventiven Bereich hat das Bundesverfassungsgericht ganz klare Grenzen gesetzt, wann es erlaubt ist, sie einzusetzen. Meine persönliche Meinung ist aber: Auch der präventive Einsatz geht schon fast zu weit.

? *Wie bewertest du, daß der bayrische Innenminister Herrmann steif und fest behauptet, der Einsatz hätte im Rahmen des Legalen stattgefunden, obwohl nachweislich Screenshots angefertigt wurden?*

Der Innenminister kann ja viel behaupten. Wenn die Software

aber nachweislich die Möglichkeit hat, illegal eingesetzt zu werden, wie will man das denn nachhalten? Da sehe ich das Problem, dass das Vertrauen der Bevölkerung in die Ermittlungsbehörden nachhaltig beeinträchtigt ist. Die Behauptung des Innenministers, die Software sei legal eingesetzt worden, die kann er gerne aufstellen, aber ob das wirklich so ist, kann ja niemand kontrollieren. Daß eine Software, die Mißbrauchspotenzial hat, auch mißbräuchlich eingesetzt wird, ist ja auch schon eindrucksvoll nachgewiesen worden. Es gab da zum Beispiel einen Fall, in dem ein Mitarbeiter einer Ermittlungsbehörde diesen Trojaner ausgenutzt hat, um seiner eigenen Frau nachzuspionieren, weil er ihr ein Verhältnis mit irgendjemandem unterstellte. Ob ein Mißbrauch stattfindet oder nicht, kann man leider nicht kontrollieren.

? *Stichwort Beweisverwendungsverbot: es ist in Deutschland ja so, dass auch illegal erlangte Beweise weiter verwendet werden können. Besteht da nicht die Gefahr, dass zum Beispiel bei einem solchen Trojaner-Einsatz die Beamten zwar wissen, dass das, was sie da tun, nicht rechtens ist, aber dass sie es insgeheim dennoch tun und die Beweise weiter verwenden?*

Ja, die Gefahr sehe ich auch. Zunächst einmal existiert in Deutschland durchaus ein Beweisverwendungsverbot, zum Beispiel für ganz krasse Rechtsbrüche bei der Beweiserlangung wie Folter. Das Problem bei unterschwellig illegal erlangten Beweisen besteht darin, dass dann durch die Gerichte eine

sogenannte Abwägung zwischen dem Strafverfolgungsinteresse und den Rechten des Beschuldigten stattfindet. Und diese Abwägung fällt in letzter Zeit immer häufiger zugunsten des staatlichen Interesses an der Strafverfolgung aus. Und das sogar bei minderschweren Straftaten. Da frage ich natürlich, in welche Richtung wir gehen. Und deswegen ist die Diskussion über ein Beweisverwendungsverbot so wichtig. Es ist immer die Frage, wie weit das gehen soll. In meiner Bachelor-Arbeit habe ich dargelegt, dass die Behörden zunehmend illegal erlangte Beweise und illegale Ermittlungsmethoden bewusst einsetzen – in dem Wissen, dass das falsch ist – weil sie ja wissen, dass die Beweise anschließend vor Gericht trotzdem eingesetzt werden können. Ich halte es für eine gefährliche Entwicklung, wenn Behörden davon ausgehen können, dass sie bei so etwas nichts zu befürchten haben und deswegen ganz bewusst illegale Methoden anwenden. Das ist eine Entwicklung, die völlig fehlt in einem Rechtsstaat, und da müssen wir unbedingt gegensteuern.

? *Nun wird immer wieder argumentiert, dass der Einsatz von Trojanern notwendig sei. Es wird hingewiesen darauf, dass zum Beispiel das normale Abhören von Telefonen immer weniger gut funktioniert, weil die Straftäter auf Internet-Telefonie ausweichen. Da kommt dann die sogenannte Quellen-TKÜ ins Spiel – also ein Euphemismus für Trojaner auf dem Rechner – die angeblich notwendig sei, um weiter Strafverfolgung betreiben zu können. Teilst Du diese Einschätzung?*

Das sehe ich differenziert. Grundsätzlich ist es vielleicht in vielen Bereichen tatsächlich notwendig, diesen Trojaner einzusetzen. Gerade im Bereich der organisierten Kriminalität, worunter man auch den Terrorismus fassen kann – da gibt es Bereiche, wo die Abschottung nach außen schon sehr stark ist, sodass solche Ermittlungsmethoden eventuell nötig sein können. Im präventiven Bereich sehe ich aber zunächst einmal überhaupt keine Notwendigkeit. Und dann ist es ja auch so, dass die Quellen-TKÜ zunehmend auch im unterschweligen Bereich zum Einsatz kommt. Also eben auch bei Straftaten unterhalb der organisierten Kriminalität. Das halte ich für völlig verfehlt.

Ein weiteres Problem besteht darin, dass eine strikte gesetzliche Regelung fehlt. Die Piratenpartei sagt ja nicht, dass sämtliche Überwachungsmaßnahmen fehl am Platz seien oder dass wir halt eine Anarchie wollen. Wir sind ja nicht polizeifeindlich oder ermittlungsfeindlich. Gerade Ermittlungsmethoden, die dermaßen tief in die Grundrechte eingreifen, müssen aber strikt gesetzlich geregelt sein und sollten ausschließlich bei einem konkreten Anfangsverdacht eingesetzt werden dürfen. Aus diesem Grund sehe ich auch eine präventive Überwachung sehr sehr kritisch. Dass der grundsätzliche Einsatz notwendig sein kann, möchte ich nicht abstreiten. Da kommen wir aber dann trotzdem in einen Bereich, wo ich frage: Wie sinnvoll ist das überhaupt? Beziehungsweise: Wie verhältnismäßig ist das? Diese Software, die jetzt eingesetzt wurde, ist schließlich dazu geeignet, tief in den Kernbereich der privaten Lebensgestaltung einzudringen. Das berührt ganz klar die



Kein Spielzeug: Bundestrojaner zum Anfassen.

Bild: mellowbox

vom Grundgesetz geschützte Menschenwürde.

Zugleich zeigt der Einsatz dieser Software aber nur Wirkung bei eher unerfahrenen Straftätern. Die echte organisierte Kriminalität weiß sich gegen so etwas längst zu wehren und abzuschotten. In dem Moment wird die Verhältnismäßigkeit äußerst problematisch. Ob man es generell ablehnen sollte, weiß ich nicht. Da muss man halt wirklich im Einzelfall schauen: Wie sinnvoll ist der Einsatz dieser Software? Aber den Einsatz ohne jeden Anfangsverdacht – den lehne ich natürlich ausnahmslos ab.

! Gut. Also Fazit: Möglicherweise in gut begründeten Ausnahmefällen, aber mit Sicherheit nicht als Regelwerkzeug der Ermittlung.

Und vor allem, also das ist ganz wichtig: Wirklich nur, also ausschließlich im Bereich schwerer Straftaten – organisierte Kriminalität und Terrorismus, bei schweren Straftaten, die das Leben oder die Freiheit betreffen. In allen Bereichen unterhalb dieser Schwelle ist ein derart schwerer Eingriff in die Grundrechte auf gar keinen Fall irgendwie zu rechtfertigen.

Alles klar. Vielen Dank für das Gespräch.

pratisch vernachlässigbare Kalkulationsgröße. Durch die in der neuen EU-Verordnung vorgesehene prozentuale Kopplung von Höchststrafen an den Unternehmensumsatz könnten diese Strafen in der Zukunft tatsächlich die erhoffte Steuerungswirkung entfalten. Mit dem Begriff ‚Gebietsbezug‘ ist hier gemeint, dass die EU-Bürger die in der Verordnung dargelegten Ansprüche grundsätzlich auch gegenüber außerhalb der EU angesiedelten Einrichtungen haben – ein Recht auf digitale Privatsphäre wird so als für die

eigenen Bürger universell angesehen und muss und kann nicht durch Verträge oder Vereinbarungen zur Datenübermittlung und -verarbeitung erst wieder jedesmal neu festgezurret werden. Flapsig gesprochen exportiert die EU damit die betroffenen Bürgerrechte zumindest für die EU-Bürger. Auch die mit einer Verordnung einhergehende europaweite Vereinheitlichung von Datenschutzstandards hat viele positive Aspekte, steht aber zu Recht auch in der kritischen Diskussion. Die Wahl einer Verordnung im Gegensatz zu einer

Richtlinie bedeutet nichts weniger als einen wichtigen Schritt in Richtung eines vereinigten Europas. Ich hoffe, dass bei der Beurteilung dieser wichtigen europäischen Datenschutzinitiative letztlich die inhaltlichen Aspekte, also die Verbesserung der Durchsetzung von Bürgerrechten, den Ausschlag geben werden.

Der Killerspiele-Killer

Die Anderen Innenminister Uwe Schünemann holzt gegen die große böse Welt und bringt Angst statt Freiheit über Niedersachsen.

Uwe Schünemann, seit 2003 Innenminister im Land Niedersachsen, präsentiert sich als Hardliner und steht für restriktive Innenpolitik. In seiner Partei, der „Christlich-Demokratischen Union“ (CDU), ist er zuständig für die Bespaßung des rechten Randes. Bei der Landtagswahl am 27. Januar 2008 gewann Direktkandidat Schünemann erneut seinen Landkreis Holzmin-

Schünemann ist ein eifriger Kämpfer für den starken Staat. Bürger- und Grundrechte kümmern ihn offensichtlich nicht so sehr. Zusammen mit IT-Großunternehmen und dem oft demagogisch agierenden Verein „Innocence in Danger“ will Schünemann das Internet säubern: „White IT“ ist sein Projekt, das er seit Jahren bei allen passenden und unpassenden Gelegenheiten ins Rampenlicht schiebt.

Eine spezielle Software soll illegale Inhalte auf dem Benutzerrechner entfernen. Zusammen mit sich „höchst geehrt“ fühlenden Fujitsu-Vertretern präsentierte er seine Technologiepartner auf der diesjährigen „Cebit“

in Hannover. Auch Internet-Provider will er nach Möglichkeit zur Filterung heranziehen.

Zu weiteren politischen Forderungen gesellen sich charmante Vorhaben wie Vorratsdatenspeicherung für „mindestens“ sechs Monate, das Verbot sogenannter „Killerspiele“, diverse Verfassungsänderungen zur leichten, routinemäßigen Rasterfahndung, großem Lauschangriff und heimlichen Hausdurchsuchungen.

Elektronische Fußfesseln für „3000 gewaltbereite Islamisten“ sollen her, und für alles, was dann noch draußen herumlungert, testete das Mitglied des Schützenvereins Holzmin den die „kommunale Bürgerstreife“ gemäß US-Vorbild. Noch ohne Schusswaffen, aber in Uniform. Der Erfolg der ehrenamtlichen 150-Euro-Streifengänger in gesetztem Alter war eher mäßig. Deshalb muss frisches Blut rekrutiert werden: Nach Auslaufen des Wehrdienstes setzt sich Schünemann für ein zwangsweises, kaserniertes „Heimatschutzjahr“ junger Männer ein. Alles heiße Luft, aus der sowie so nichts wird, da Realität oder



Bild: Martina Nolte (BY-SA-3.0)

Uwe Schünemann, Innenminister von Niedersachsen

Verfassungsgericht die Projekte ausbremsen.

Lieblingsopfer seiner Demagogie ist die liberale Bundesjustizministerin Leutheusser-Schnarrenberger. Sie lässt nach seinen Worten eine „Schutzlücke“ weit offen, denn sie stimmt der Vorratsdatenspeicherung bisher nicht zu. Doch die größte Schutzlücke öffnet der Minister selbst: er macht mit seinem Herumgehölze rechtsradikale Ideologie erst recht salonfähig.